HKUST – Department of Computer Science and Engineering
COMP 2711: Discrete Math Tools for CS – Spring 2012

Midterm Examination 1

#

Date: Friday, March 2, 2012 Time: 19:00–21:00

Name: _____	Student ID: _____
Email: _____	Lecture and Tutorial: _____

Instructions

- This is a closed book exam. It consists of 13 pages and 8 questions.
- Please write your name, student ID, email, lecture section and tutorial on this page.
- For each subsequent page, please write your student ID at the top of the page in the space provided.
- Please sign the honor code statement on page 2.
- Answer all the questions within the space provided on the examination paper. You may use the back of the pages for your rough work. The last three pages are scrap paper and may also be used for rough work. Each question is on a separate page. This is for clarity and is not meant to imply that each question requires a full page answer. Many can be answered using only a few lines.
- **Unless otherwise specified you *must* always explain how you derived your answer. A number without an explanation will be considered an incorrect answer.**
- Solutions can be written in terms of binomial coefficients and falling factorials. For example, $\binom{5}{3} + \binom{4}{2}$ may be written instead of 16, and $5^{\underline{3}}$ instead of 60. Calculators may be used for the exam (but are not necessary).
- Please *do not* use the ${}_nP_k$ and ${}_nC_k$ notation. Use $n^{\underline{k}}$ and $\binom{n}{k}$ instead.

Questions	1	2	3	4	5	6	7	8	Total
Points	15	16	14	10	10	12	14	9	100
Score									

Student ID: _____

As part of HKUST's introduction of an honor code, the HKUST Senate has recommended that all students be asked to sign a brief declaration printed on examination answer books that their answers are their own work, and that they are aware of the regulations relating to academic integrity. Following this, please read and sign the declaration below.

I declare that the answers submitted for this examination are my own work.

I understand that sanctions will be imposed, if I am found to have violated the University regulations governing academic integrity.

Student's Name: _____

Student's Signature: _____

Student ID: _____

Problem 1: [15 points]
Suppose six persons $\{p_1, p_2, p_3, p_4, p_5, p_6\}$ are to be seated in a row of 6 seats facing the same direction.

(a) How many ways are there to seat the 6 persons such that p_5 must sit to the left of p_6? (e.g. $(p_1, \mathbf{p_5}, p_3, p_2, \mathbf{p_6}, p_4)$ is valid, but $(p_1, p_3, \mathbf{p_6}, \mathbf{p_5}, p_2, p_4)$ is invalid)

(b) How many ways are there to seat everyone if p_4 and p_5 must both sit to the left of p_6?

(c) Consider n people $\{p_1, p_2, \cdots, p_n\}$ to be seated in a row of n seats where $n > 1$. How many different ways are there to seat them if $p_1, p_2, \cdots, p_k$ must sit to the left of p_{k+1}, where $1 \leq k < n$?

Solution:

(a) $6!/2$. There are a total $6!$ seating arrangements, only half of them are valid.

(b) $6!/3$. There are a total $6!$ seating arrangements, only one-third of them are valid. To see this, consider seating p_4, p_5 and p_6 at three fixed seats. The are totally $3!$ ways. Among them, there are $2!$ ways where p_6 sits at the right most seat. The ratio is $2!/3! = 1/3$.

(c) $n!/(k+1)$. There are a total $n!$ seating arrangements, only $1/(k+1)$ of them are valid. To see this, consider seating p_1, $\cdots$, p_{k+1} at $k+1$ fixed seats. The are totally $(k+1)!$ ways. Among them, there are $k!$ ways where p_{k+1} sits at the right most seat. The ratio is $k!/(k+1)! = 1/(k+1)$.

Grading: 5 points each.

Student ID: _____

Problem 2: [16 points]
Consider $S_m = \{1, 2, 3, \ldots, m\}$ and $S_n = \{1, 2, 3, \ldots, n\}$ with $m, n \geq 3$.

(a) How many functions f are there from S_m to S_n such that $f(x) = 1$ for at least one $x \in S_m$?

(b) How many functions f are there from S_m to S_n such that $f(x) \in \{1, 2\}$ for at least one $x \in S_m$?

(c) How many functions f are there from S_m to S_n such that $f(x) = 1$ for at least one $x \in S_m$ **and** $f(y) \neq 2$ for any $y \in S_m$?

(d) How many functions f are there from S_m to S_n such that $f(x) = 1$ for at least one $x \in S_m$ **and** $f(y) = 2$ for at least one $y \in S_m$?

Solution:

(a) $n^m - (n-1)^m$: There are totally n^m functions and there are $(n-1)^m$ functions from S_m to $\{2, 3, \ldots, n\}$. The difference is that number of functions such that $f(x) = 1$ for at least one $x \in S_m$.

(b) $n^m - (n-2)^m$: There are totally n^m functions and there are $(n-2)^m$ functions from S_m to $\{3, \ldots, n\}$.

(c) $(n-1)^m - (n-2)^m$: This is the same as (a) except that we cannot use $2 \in S_n$ as a function value.

(d) $(n^m - (n-2)^m) - 2((n-1)^m - (n-2)^m)$: The number for (b) − the number for (c) − the number of functions such that $f(x) \neq 1$ for any $x \in S_m$ **and** $f(y) = 2$ for at least one $y \in S_m$.

Grading: 4 points each.

Student ID: _____

Problem 3: [14 points]
Let m and n be two positive integers. Give a combinatorial proof for the following equation:

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{n}{k}\binom{m}{r-k}$$

Remark: This identity was discovered by Alexandre-Theophile Vandermonde in the eighteenth century and, thus, it is known as **Vandermonde's identity**.

Solution:

Suppose we wish to count the number of ways to choose r items from the union of two sets, where the first set contains m items and the second set contains n items.

The left-hand side of the identity calculates this number by first taking the union of the two sets, which contains $m + n$ items, and then taking all possible choices of r items from this set.

The right-hand side of the identify calculates the same number, but in a different way. Specifically, it first selects k items from the first set that contains n items, and then chooses $r - k$ items from the second set that contains m items. The final summation stems from the fact that (i) k ranges from 0 to r, and (ii) by the Sum Principle (since we can either select 0 items from the first set and r items from the second, or 1 item from the first and $r - 1$ from the second, etc.).

Grading: 6 for the setup, 3 for left hand side, 5 for right hand side. Probably, full points or nothing in most cases.

Student ID: _____

Problem 4: [10 points] Let n, k_1, k_2, k_3 and k_4 be nonnegative integers such that $k_1 + k_2 + k_3 + k_4 = n$. Consider expanding the expression

$$(w + x + y + z)^n.$$

What is the coefficient for the following term in the expansion

$$w^{k_1} x^{k_2} y^{k_3} z^{k_4}?$$

Justify your answer.

Solution:

$$\frac{n!}{k_1!k_2!k_3!k_4!}$$

The expression expands into 4^n monomial terms, each with n positions. The coefficient is the same as the number of ways to place w at k_1 positions, x to k_2 positions, y to k_3 positions, and z to k_4 positions:

$$\binom{n}{k_1}\binom{n-k_1}{k_2}\binom{n-k_1-k_2}{k_3} = \frac{n!}{k_1!k_2!k_3!k_4!}$$

Grading: 5 for correct answer, and 5 for justification.

Student ID: _____

Problem 5: [10 points]
Find $gcd(168, 567)$ by running the GCD algorithm on paper. Show all the intermediate steps.

Solution:

$$gcd(567, 168) = gcd(168, 63) \quad 56 = 3 \times 168 + 63$$
$$gcd(168, 63) = gcd(63, 42) \quad 168 = 2 \times 63 + 42$$
$$gcd(63, 42) = gcd(42, 21) \quad 63 = 1 \times 42 + 21$$
$$gcd(42, 21) = gcd(21, 0) = \mathbf{21} \quad 42 = 2 \times 21 + 0$$

So, $gcd(168, 567) = 21$.

Grading: 2 for each step, and 2 for the final answer.

Student ID: _____

Problem 6: [12 points]
Consider encrypting messages written in capital letters of the English alphabet. We represent 'A' as '0', 'B' as '1', and so on. Suppose the following function is used for encryption:

$$f_{3,26}(x) = (x \cdot 3) \bmod 26.$$

What is the ciphertext for the message "I LOVE MATH"? Show: (1) the original message in integers, (2) the ciphertext in intgers, and (3) the ciphertext in capital letters.

Solution:

- Original message in integers: 8 11-14-21-4 12-0-19-7
- Ciphertext in integers: 24 7-16-11-12 10-0-5-21
- Ciphertext in Capital letters: Y HQLM KAFV

Grading: -1 for each mistake

Student ID: _____

Problem 7: [14 points]
Let a, b, m and n be positive integers. Suppose

$$a \bmod m = b \bmod m, \quad n|m.$$

Prove the following equations:

(a) $a \bmod n = b \bmod n$.

(b) $a^2 \bmod m = b^2 \bmod m$.

Solution:

(a) Since $n|m$, it holds that $m = tn$ for some integer t. Moreover, $a \bmod m = b \bmod m$ implies $(a - b) \bmod m = 0$, which in turn implies there exists integer q such that

$$\begin{aligned}(a-b) &= qm \\ \Rightarrow (a-b) &= qtn.\end{aligned}$$

So n divides $(a-b)$. This implies $(a-b) \bmod n = 0$, which in turn implies $a \bmod n = b \bmod n$.

(b) As shown earlier, $(a - b) = qm$ for some q. Multiplying both sides with $(a + b)$, we get

$$a^2 - b^2 = (a+b)(a-b) = (a+b)qm.$$

So m divides $a^2 - b^2$. This implies that $a^2 - b^2 \bmod m = 0$, which in turn implies that $a^2 \bmod m = b^2 \bmod m$.

Grading: 7 points each

Student ID: _____

Problem 8: [9 points]
Prove that 21 does not have an inverse in Z_{111}.

Solution: Consider the following equation:

$$(21 \cdot x) \bmod 111 = 1$$

We have

$$\begin{aligned} 1 &= (21 \cdot x) \bmod 111 \\ \Rightarrow 1 &= 21 \cdot x - 111q \\ \Rightarrow 1 &= 3(7 \cdot x - 37q) \end{aligned}$$

Since 3 does not divide 1, the equation has no solution. Therefore, 21 does not have an inverse in Z_{111}.

Grading: Deduct points for mistakes. Probably full marks or nothing in most cases.

Student ID: _____

Scrap Paper

Student ID: _____

Scrap Paper

Student ID: _____

Scrap Paper